In the Specification

On page 1, after line 3 (before line 4), please insert the heading and the subheading:

BACKGROUND OF THE INVENTION

On page 3, after line 4 (between the first and second paragraphs), please insert the heading:

SUMMARY OF THE INVENTION

On page 11, after line 10, please insert the heading and the following paragraphs:

BRIEF DESCRIPTION OF THE DRAWINGS

Figures 1A shows the function "raise to the square in CG(p)" by an oriented graph in the case where p is congruent to 3 (mod 4).

Figures 1B shows the function "raise to the square in CG(p)" by an oriented graph in the case where p is congruent to 5 (mod 8).

Figures 1C shows the function "raise to the square in CG(p)" by an oriented graph in the case where p is congruent to 9 (mod 16).

Figures 1D shows the function "raise to the square in CG(p)" by an oriented graph in the case where p is congruent to 17 (mod 32).

Figure 2 shows the solutions to the equation (3.a) with $k = 6$ and p congruent to 5 (mod 8), giving $t = 2$.

Figure 3 shows $G_i = g_i^2$ in a cycle with a prime factor p congruent to 9 (mod 16).

Figure 4 shows $G_i = g_i^2$ on a branch with a prime factor p congruent to 65 (mod 128).

On page 12, please replace line 1 with the heading:

DETAILED DESCRIPTION OF THE INVENTION

On page 17, please replace the third paragraph with the following rewritten paragraph:

Figures 1A to 1D illustrate the function "raise to the square in CG(p)" by an oriented graph where each of the p–1 non-zero elements of the field finds its place: the non-quadratic residues 1 are in white and the quadratic residues 5 are in black; among the quadratic residues 5, the odd-parity ranking elements 3 are in circles.

On pages 19-20, please replace the last paragraph of page 19 and the first paragraph of page 20 with the following rewritten paragraph:

When $t = 1$, p is congruent to 3 (mod 4) as shown in Figure 1A. The Legendre symbols of g and $-g$ with respect to p are different: any quadratic residue of CG(p) has two square roots in CG(p): one is a quadratic residue and the other is a non-quadratic residue. Firstly, one of the two equations (1.a) or (2.a) has two solutions in x in CG(p) and the other does not have any. Secondly, the equation (3.a) has two solutions in x in CG(p) whatever the value of k.

On page 20, please replace the second paragraph with the following rewritten paragraph:

When $t = 2$, p is congruent to 5 (mod 8) as shown in Figure 1B. Two cases occur, depending on the Legendre symbol of g with respect to p. When the symbol is equal to -1, g and $-g$ are both non-quadratic residues of CG(p): the three equations (1.a), (2.a) and (3.a) have no solution in x in CG(p). When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of CG(p), each equation (1.a) and (2.a) has two solutions in x in CG(p). Furthermore, the rank of g^2 in CG(p) is an odd-parity value implying that whatever the value of k, the equation (3.a) has four solutions in x in CG(p) of which only one has an odd-parity rank.

On pages 20-21, please replace the last paragraph of page 20 and the first paragraph of page 21 with the following rewritten paragraph:

When $t = 3$, p is congruent to 9 (mod 16) <u>as shown in Figure 1C</u>. Let us consider the Legendre symbol of g with respect to p. When the symbol is equal to -1, g and $-g$ are two non-quadratic residues of CG(p): the three equations (1.a), (2.a) and (3.a) have no solution in x in CG(p). When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of CG(p); each equation (1.a) and (2.a) has two solutions in x in CG(p). The existence of solutions in x to the equation (3.a) depends on the rank of g^2 in CG(p). This rank is an odd-parity value or is divisible by two but not by four. When the rank of g^2 in CG(p) is divisible by two but not by four, the equation (3.a) has four solutions in x in CG(p) for $k = 2$; it cannot go above $k \geq 3$. When the rank of g^2 in CG(p) is an odd-parity value, the equation (3.a) has four solutions in x in CG(p) for $k = 2$ and eight for $k \geq 3$. In both cases, only one value is an odd-parity value.

On page 21, please replace the second paragraph with the following rewritten paragraph:

When $t = 4$, p is congruent to 17 (mod 32) <u>as shown in Figure 1D</u>. Let us consider the Legendre symbol of g with respect to p. When the symbol is equal to -1, g and $-g$ are two non-quadratic residues of CG(p): the three equations (1.a), (2.a) and (3.a) have no solution in x in CG(p). When the symbol is equal to $+1$, g and $-g$ are two quadratic residues of CG(p); each equation (1.a) and (2.a) has two solutions in x in CG(p). The existence of solutions in x to the equation (3.a) depends on the rank of g^2 in CG(p). This rank is an odd-parity value or is divisible by two or four but not by eight. When the rank of g^2 in CG(p) is divisible by two but not by eight, the equation (3.a) has four solutions in x in CG(p) for $k = 2$; it cannot go above $k \geq 3$. When the rank of g^2 in CG(p) is divisible by two but not by four, the equation (3.a) has four solutions in x in CG(p) for $k = 2$ or eight for $k = 3$; it has no solutions for $k \geq 4$. When the rank of g^2 in CG(p) is an odd-parity value, the equation (3.a) has four solutions in x in CG(p) for $k = 2$ and eight for $k \geq 3$ and sixteen for $k \geq 4$. In all three cases, only one value is an odd-parity value.